What Is Claimed Is:

1. A method for preventing unauthorized access into a computer unit using a personal identification device and an input and output (I/O) control chip to control the activation of the computer unit, the steps comprising of:

(a) said personal identification device entering into a standby status;

(b) inputting personal identification data into said personal identification device;

(c) determining the validity of said personal identification data and returning to said step (a) if said personal identification data is invalid;

(d) said personal identification device activating a control circuit, which allows said I/O control chip to activate a computer keyboard and displaying a notification message prompting an authorized user to enter a password;

(e) said authorized user entering said password;

(f) said I/O control chip determining validity of said password and returning to said step (e) if said password is invalid;

(g) said I/O control chip activating said computer unit;

(h) said computer unit returns to normal operations;

(i) searching for said personal identification data in said personal identification device, and jumping to step (n) if said personal identification data are found;

(j) said personal identification device activating a suspend function in said computer unit to stop all I/O operations, and informing said suspension to said authorized user through a personal identification data display;

(k) searching for new personal identification data and returning to step (j) if not found;

(l) determining the validity of said new personal identification data and returning to said step (j) if invalid;

(m) said personal identification device deactivating said suspend function and returning to step (h); and

(n) returning to normal operations for said computer unit.

2. The method of claim 1, further includes the steps of :

(o) searching for said personal identification data in a preset time period and jumping to step (q) if not found;

(p) triggering an alarm through said personal identification device and returning to step (o); and

(q) said identification device returning to a standby status.

3. The method of claim 1, wherein said personal identification device is a card reader.

4. The method of claims 1, wherein said personal identification data are derived from an IC card.

5. The method of claim 1, wherein said personal identification data display is an LED.

6. The method of claim 2, wherein said preset time period is set for 10 seconds.

7. An apparatus for a computer unit security system comprising:

personal identification data for use by a personal identification device for identifying an authorized user; and

said personal identification device having an I/O control circuit connected to said computer unit as to allow normal operations when said authorized user is identified, suspending all operations of said computer unit when said personal identification data are removed prior to said computer unit being shut down, and preventing said computer unit from reactivation if said personal identification data is not revalidated, wherein said computer unit comprises:

a processor;

a North Bridge chip connected to said processor for controlling data flow between said processor and a PCI and allowing said processor to retrieve or save files from at least a memory and AGP;

a South Bridge chip connected to said North Bridge chip and an I/O control chip and serving as a bridge between a USB interface and said I/O control device;

said I/O control chip connected to said South Bridge chip for activating said computer unit after receiving a valid password inputted through a keyboard; and

said keyboard connected to said personal identification device and said I/O control chip which activates said keyboard for inputting said valid password after said authorized user has been identified.

8. The apparatus of claim 7, wherein said personal identification device includes an LED.

9. The apparatus of claim 7, wherein said personal identification device includes a timer for reminding said authorized user regarding the non-removal of said personal identification data within a preset time period after said computer unit has been deactivated.

10. The apparatus of claim 7, wherein said preset time period is set for 10 seconds.

11. The apparatus of claim 7, wherein said personal identification device is a reader.

12. The apparatus of claim 7, wherein said personal identification data are derived from an IC card.